GENUS TWO CURVES COVERING ELLIPTIC CURVES: A COMPUTATIONAL APPROACH

T. SHASKA

Abstract. A genus 2 curve C has an elliptic subcover if there exists a degree n maximal covering $\psi : C \to E$ to an elliptic curve E. Degree n elliptic subcovers occur in pairs (E, E'). The Jacobian J_C of C is isogenous of degree n^2 to the product $E \times E'$. We say that J_C is (n, n)-split. The locus of C, denoted by $\mathcal{L}_n$, is an algebraic subvariety of the moduli space $\mathcal{M}_2$. The space $\mathcal{L}_2$ was studied in Shaska/Völklein [32] and Gaudry/Schost [10]. The space $\mathcal{L}_3$ was studied in [26] were an algebraic description was given as sublocus of $\mathcal{M}_2$.

In this survey we give a brief description of the spaces $\mathcal{L}_n$ for a general n and then focus on small n. We describe some of the computational details which were skipped in [32] and [26]. Further we explicitly describe the relation between the elliptic subcovers E and E'. We have implemented most of these relations in computer programs which check easily whether a genus 2 curve has $(2, 2)$ or $(3, 3)$ split Jacobian. In each case the elliptic subcovers can be explicitly computed.

1. Introduction

Let C be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. Let $\psi : C \to E$ be a degree n maximal covering (i.e. does not factor through an isogeny) to an elliptic curve E defined over k. We say that C has a *degree n elliptic subcover*. Degree n elliptic subcovers occur in pairs. Let (E, E') be such a pair. It is well known that there is an isogeny of degree n^2 between the Jacobian J_C of C and the product $E \times E'$. We say that C has **(n,n)-split Jacobian**. The locus of such C, denoted by $\mathcal{L}_n$, is a 2-dimensional algebraic subvariety of the moduli space $\mathcal{M}_2$ of genus two curves.

In this survey we study the genus 2 curves with (n, n)-split Jacobian for small n. While such curves have been studied by many authors, our approach is simply computational. Some of the results have appeared in previous articles of the author.

Curves of genus 2 with elliptic subcovers go back to Legendre and Jacobi. Legendre, in his *Théorie des fonctions elliptiques*, gave the first example of a genus 2 curve with degree 2 elliptic subcovers. In a review of Legendre's work, Jacobi (1832) gives a complete description for $n = 2$. The case $n = 3$ was studied during the 19th century from Hermite, Goursat, Burkhardt, Brioschi, and Bolza. For a history and background of the 19th century work see Krazer [19, pg. 479]. Cases when $n > 3$ are more difficult to handle. Frey and Kani note the difficulty to get explicit examples, see Frey [8] and Frey, Kani [9].

In §2 we give a brief description of genus 2 curves and their isomorphism classes which are classified by the absolute invariants of binary sextics. Further, we display the list of groups that occur as full automorphism groups of genus 2 curves defined over a field of characteristic $\neq 2$.

In §3 we study degree n covers $\mathcal{C} \to E$ from a genus 2 curve to an elliptic curve. Such covers induce a degree n covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$. A careful study of such covers leads to determining an equation for the curves $\mathcal{C}$. The covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ could have different ramification structure. All such structures are described in section 3.

The moduli space of coverings $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ with fixed ramification structure is a Hurwitz space. The irreducibility of such space, dimension, and the genus (in the case 1-dimensional spaces) can be computed via the braid action. For n an odd integer we display such results in section 4. There is a natural morphism between the Hurwitz space and the locus $\mathcal{L}_n$ (cf. §4). In the second part of section 4 we describe the correspondence between the points of $\mathcal{L}_n$ and the Humbert space of discriminant n^2 which we denote by $\mathcal{H}_{n^2}$.

In section 5 we study genus 2 curves with degree 2 elliptic subcovers. Jacobi [16] gives a general form of such curves: $Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1$, and a description of $\mathcal{L}_2$ in terms of the cross ratios of the roots $\alpha_1, \dots, \alpha_6$ of the sextic:

$$\frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2} : \frac{\alpha_4 - \alpha_1}{\alpha_4 - \alpha_2} = \frac{\alpha_5 - \alpha_1}{\alpha_5 - \alpha_2} : \frac{\alpha_6 - \alpha_1}{\alpha_6 - \alpha_2}$$

Thus, $\mathcal{L}_2$ is parameterized by the pair $(s_1, s_2) \in k^2$. We note that this parametrization of $\mathcal{L}_2$ factors through a ramified Galois covering: $k^2 \longrightarrow k^2$, $(s_1, s_2) \to (u, v)$, where $u = s_1 s_2$ and $v = s_1^3 + s_2^3$. This induces a birational parametrization of $\mathcal{L}_2$ by the pairs (u, v). All our computations use these coordinates (u, v). We use this to compute an equation for $\mathcal{L}_2$ in terms of the classical invariants. We give a general relation between the j-invariants of degree 2 elliptic subfields of K. This improves [10], where each isomorphism type of G is treated separately. We determine conditions when degree 2 elliptic subfields of K are 2 or 3-isogenous. For a generalization of such invariants u, and v see Remark 1 or Gutierrez/Shaska [10].

In section 6, we study the case $n = 3$. We show that every genus 2 curve with a degree 3 elliptic subcover can be written in the form

$$Y^2 = (X^3 + aX^2 + bX + 1)(4X^3 + b^2 X^2 + 2bX + 1)$$

for $a, b \in k$. So $\mathcal{L}_3$ is parameterized by the pairs $(a, b) \in k^2$. The invariants of the two cubics r_1, r_2 give a birational parametrization of $\mathcal{L}_3$. This parametrization of $\mathcal{L}_3$ factors through ramified Galois coverings of degree 3 (resp. 2)

$$\begin{aligned} k^2 &\to k^2 \to k^2 \\ (a, b) &\to (u, v) \to (r_1, r_2) \end{aligned} \tag{1}$$

where $ab = u$ and $b^3 = v$. The equation of $\mathcal{L}_3$ is computed in terms of the absolute invariants and is displayed in [26, Appendix A]. If $\mathcal{C} \in \mathcal{L}_3$ then $Aut(\mathcal{C})$ is isomorphic to $\mathbb{Z}_2, V_4,\ D_4$ or D_6. Moreover, there are exactly six genus 2 curves with automorphism group D_4 or D_6. The rational models of these 12 curves and rational points on them were studied in [29]. We determine the j-invariants of the elliptic subcovers and show that they satisfy the Fricke polynomial of level 2.

In the last section we give information on computer programs that we have made available for such computations.

2. Preliminaries

Let k be an algebraically closed field of characteristic zero and C a genus 2 curve defined over k. Then C can be described as a double cover of $\mathbb{P}^1(k)$ ramified in 6 places $w_1, \dots, w_6$. This sets up a bijection between isomorphism classes of genus 2 curves and unordered distinct 6-tuples $w_1, \dots, w_6 \in \mathbb{P}^1(k)$ modulo automorphisms of $\mathbb{P}^1(k)$. An unordered 6-tuple $\{w_i\}_{i=1}^6$ can be described by a binary sextic (i.e. a homogenous equation $f(X, Z)$ of degree 6). Let $\mathcal{M}_2$ denote the moduli space of genus 2 curves. To describe $\mathcal{M}_2$ we need to find polynomial functions of the coefficients of a binary sextic $f(X, Z)$ invariant under linear substitutions in X, Z of determinant one. These invariants were worked out by Clebsch and Bolza in the case of zero characteristic and generalized by Igusa for any characteristic different from 2; see [3], [15], or [32] for a more modern treatment.

Consider a binary sextic, i.e. a homogeneous polynomial $f(X, Z)$ in $k[X, Z]$ of degree 6:

$$f(X, Z) = a_6X^6 + a_5X^5Z + \cdots + a_0Z^6.$$

Igusa J-invariants $\{J_{2i}\}$ of $f(X, Z)$ are homogeneous polynomials of degree $2i$ in $k[a_0, \dots, a_6]$, for $i = 1, 2, 3, 5$; see [15], [32] for their definitions. Here J_{10} is simply the discriminant of $f(X, Z)$. It vanishes if and only if the binary sextic has a multiple linear factor. These J_{2i} are invariant under the natural action of $SL_2(k)$ on sextics. Dividing such an invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

Two genus 2 fields K (resp., curves) in the standard form $Y^2 = f(X, 1)$ are isomorphic if and only if the corresponding sextics are $GL_2(k)$ conjugate. Thus if I is a $GL_2(k)$ invariant (resp., homogeneous $SL_2(k)$ invariant), then the expression $I(K)$ (resp., the condition $I(K) = 0$) is well defined. Thus the $GL_2(k)$ invariants are functions on the moduli space $\mathcal{M}_2$ of genus 2 curves. This $\mathcal{M}_2$ is an affine variety with coordinate ring

$$k[\mathcal{M}_2] = k[a_0, \dots, a_6, J_{10}^{-1}]^{GL_2(k)}$$

which is the subring of degree 0 elements in $k[J_2, \dots, J_{10}, J_{10}^{-1}]$. The *absolute invariants*

$$i_1 := 144\frac{J_4}{J_2^2}, \; i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \; i_3 := 486\frac{J_{10}}{J_2^5},$$

are even $GL_2(k)$-invariants. Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. If $J_2 = 0$ then we can define new invariants as in [27]. For the rest of this paper if we say "there is a genus 2 curve $\mathcal{C}$ defined over k" we will mean the k-isomorphism class of $\mathcal{C}$. We have the following; see [32, Theorem 2].

Lemma 1. *The automorphism group G of a genus 2 curve $\mathcal{C}$ in characteristic $\neq 2$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_8, D_{12}, $\mathbb{Z}_3 \rtimes D_8$, $GL_2(3)$, or 2^+S_5. The case when $G \cong 2^+S_5$ occurs only in characteristic 5. If $G \cong \mathbb{Z}_3 \rtimes D_8$ (resp., $GL_2(3)$) then $\mathcal{C}$ has equation $Y^2 = X^6 - 1$ (resp., $Y^2 = X(X^4 - 1)$). If $G \cong \mathbb{Z}_{10}$ then $\mathcal{C}$ has equation $Y^2 = X^6 - X$.*

3. Curves of genus 2 with split Jacobians

Let C and E be curves of genus 2 and 1, respectively. Both are smooth, projective curves defined over k, $char(k) = 0$. Let $\psi : C \longrightarrow E$ be a covering of degree

n. From the Riemann-Hurwitz formula, $\sum_{P\in C}(e_\psi(P)-1)=2$ where $e_\psi(P)$ is the ramification index of points $P\in C$, under ψ. Thus, we have two points of ramification index 2 or one point of ramification index 3. The two points of ramification index 2 can be in the same fiber or in different fibers. Therefore, we have the following cases of the covering ψ:

Case I: There are $P_1,\ P_2\in C$, such that $e_\psi(P_1)=e_\psi(P_2)=2$, $\psi(P_1)\neq\psi(P_2)$, and $\forall P\in C\setminus\{P_1,P_2\}$, $e_\psi(P)=1$.
Case II: There are $P_1,\ P_2\in C$, such that $e_\psi(P_1)=e_\psi(P_2)=2$, $\psi(P_1)=\psi(P_2)$, and $\forall P\in C\setminus\{P_1,P_2\}$, $e_\psi(P)=1$.
Case III: There is $P_1\in C$ such that $e_\psi(P_1)=3$, and $\forall P\in C\setminus\{P_1\}$, $e_\psi(P)=1$.

In case I (resp. II, III) the cover ψ has 2 (resp. 1) branch points in E.

Denote the hyperelliptic involution of C by w. We choose $\mathcal{O}$ in E such that w restricted to E is the hyperelliptic involution on E. We denote the restriction of w on E by v, $v(P)=-P$. Thus, $\psi\circ w=v\circ\psi$. E[2] denotes the group of 2-torsion points of the elliptic curve E, which are the points fixed by v. The proof of the following two lemmas is straightforward and will be omitted.

Lemma 2. *a) If $Q\in E$, then $\forall P\in\psi^{-1}(Q)$, $w(P)\in\psi^{-1}(-Q)$.*
b) For all $P\in C$, $e_\psi(P)=e_\psi(w(P))$.

Let W be the set of points in C fixed by w. Every curve of genus 2 is given, up to isomorphism, by a binary sextic, so there are 6 points fixed by the hyperelliptic involution w, namely the Weierstrass points of C. The following lemma determines the distribution of the Weierstrass points in fibers of 2-torsion points.

Lemma 3. *The following hold:*
1. $\psi(W)\subset E[2]$
2. *If n is an odd number then i) $\psi(W)=E[2]$ ii) If $Q\in E[2]$ then $\#(\psi^{-1}(Q)\cap W)=1 \mod (2)$*
3. *If n is an even number then for all $Q\in E[2]$, $\#(\psi^{-1}(Q)\cap W)=0 \mod (2)$*

Let $\pi_C: C\longrightarrow\mathbb{P}^1$ and $\pi_E: E\longrightarrow\mathbb{P}^1$ be the natural degree 2 projections. The hyperelliptic involution permutes the points in the fibers of π_C and π_E. The ramified points of π_C, π_E are respectively points in W and $E[2]$ and their ramification index is 2. There is $\phi:\mathbb{P}^1\longrightarrow\mathbb{P}^1$ such that the diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ \psi\downarrow & & \downarrow\phi \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array} \tag{2}$$

Next, we will determine the ramification of induced coverings $\phi:\mathbb{P}^1\longrightarrow\mathbb{P}^1$. First we fix some notation. For a given branch point we will denote the ramification of points in its fiber as follows. Any point P of ramification index m is denoted by (m). If there are k such points then we write $(m)^k$. We omit writing symbols for unramified points, in other words $(1)^k$ will not be written. Ramification data between two branch points will be separated by commas. We denote by $\pi_E(E[2])=\{q_1,\dots,q_4\}$ and $\pi_C(W)=\{w_1,\dots,w_6\}$.

3.0.1. *The Case When n is Odd.* The following theorem classifies the ramification types for the induced coverings $\phi:\mathbb{P}^1\longrightarrow\mathbb{P}^1$ when the degree n is odd.

Theorem 1. *Let $\psi : C \longrightarrow E$ be a covering of odd degree n and $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be the induced covering induced by ψ. This induces a partitioning of the set of 6 Weierstrass points of C into two sets $W^{(1)} = W^{(1)}(C, E)$ and $W^{(2)} = W^{(2)}(\mathcal{C}, E)$, each of cardinality 3 such that $|\phi(W^{(1)})| = 1$ and $|\phi(W^{(2)})| = 3$. Then the ramification structure of ϕ is as follows.*

Case I: *(the generic case)*

$$\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-3}{2}}, (2)^1\right)$$

Or the following degenerate cases:

Case II: *(the 4-cycle case and the dihedral case)*

i) $\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (4)^1(2)^{\frac{n-7}{2}}\right)$

ii) $\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}\right)$

iii) $\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (4)^1(2)^{\frac{n-5}{2}}, (2)^{\frac{n-3}{2}}\right)$

Case III: *(the 3-cycle case)*

i) $\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (3)^1(2)^{\frac{n-5}{2}}\right)$

ii) $\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (3)^1(2)^{\frac{n-3}{2}}, (2)^{\frac{n-3}{2}}\right)$

3.0.2. *The Case When n is Even.* Let us assume now that $deg(\psi) = n$ is an even number. The following theorem classifies the induced coverings in this case.

Theorem 2. *If n is an even number then the generic case for $\psi : C \longrightarrow E$ induce the following three cases for $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$:*

I: $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

II: $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

III: $\left((2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

Each of the above cases has the following degenerations (two of the branch points collapse to one)

I: (1) $\left((2)^{\frac{n}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\right)$

(2) $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}\right)$

(3) $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-4}{2}}\right)$

(4) $\left((3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\right)$

II: (1) $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(2) $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(3) $\left((4)(2)^{\frac{n-8}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(4) $\left((2)^{\frac{n-4}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(5) $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}\right)$

(6) $\left((3)(2)^{\frac{n-6}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(7) $\left((2)^{\frac{n-4}{2}}, (3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

III: (1) $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n}{2}}\right)$

(2) $\left((2)^{\frac{n-6}{2}}, (4)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(3) $\left((2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n-10}{2}}\right)$

(4) $\left((3)(2)^{\frac{n-8}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

3.1. **Maximal coverings $\psi : C \longrightarrow E$.** Let $\psi_1 : C \longrightarrow E_1$ be a covering of degree n from a curve of genus 2 to an elliptic curve. The covering $\psi_1 : C \longrightarrow E_1$ is called a **maximal covering** if it does not factor through a nontrivial isogeny. A map of algebraic curves $f : X \to Y$ induces maps between their Jacobians $f^* : J_Y \to J_X$ and $f_* : J_X \to J_Y$. When f is maximal then f^* is injective and $ker(f_*)$ is connected, see [30] for details.

Let $\psi_1 : C \longrightarrow E_1$ be a covering as above which is maximal. Then ${\psi^*}_1 : E_1 \to J_C$ is injective and the kernel of $\psi_{1,*} : J_C \to E_1$ is an elliptic curve which we denote by E_2; see [9] or [21]. For a fixed Weierstrass point $P \in C$, we can embed C to its Jacobian via

$$
\begin{aligned}
i_P : C &\longrightarrow J_C \\
x &\to [(x) - (P)]
\end{aligned}
\tag{3}
$$

Let $g : E_2 \to J_C$ be the natural embedding of E_2 in J_C, then there exists $g_* : J_C \to E_2$. Define $\psi_2 = g_* \circ i_P : C \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} J_C \xrightarrow{\psi_{1,*}} E_1 \to 0$$

The dual sequence is also exact

$$0 \to E_1 \xrightarrow{\psi_1^*} J_C \xrightarrow{g_*} E_2 \to 0$$

If $deg(\psi_1)$ is an odd number then the maximal covering $\psi_2 : C \to E_2$ is unique (up to isomorphism of elliptic curves), see Kuhn [21]. If the cover $\psi_1 : C \longrightarrow E_1$ is given, and therefore ϕ_1, we want to determine $\psi_2 : C \longrightarrow E_2$ and ϕ_2. The study of the relation between the ramification structures of ϕ_1 and ϕ_2 provides information in this direction. The following lemma (see [9, pg. 160]) answers this question for the set of Weierstrass points $W = \{P_1, \dots, P_6\}$ of C when the degree of the cover is odd.

Lemma 4. *Let $\psi_1 : C \longrightarrow E_1$, be maximal of degree n. Then, the map $\psi_2 : C \to E_2$ is a maximal covering of degree n. Moreover,*

i) *if n is odd and $\mathcal{O}_i \in E_i[2]$, $i = 1, 2$ are the places such that $\#(\psi_i^{-1}(\mathcal{O}_i) \cap W) = 3$, then $\psi_1^{-1}(\mathcal{O}_1) \cap W$ and $\psi_2^{-1}(\mathcal{O}_2) \cap W$ form a disjoint union of W.*

ii) *if n is even and $Q \in E[2]$, then $\#\left(\psi^{-1}(Q)\right) = 0$ or 2.*

The above lemma says that if ψ is maximal of even degree then the corresponding induced covering can have only type **I** ramification, see theorem 2.

4. The locus of genus two curves with (n, n) split Jacobians

In this section we will discuss the Hurwitz spaces of coverings with ramification as in the previous section and the Humbert spaces of discriminant n^2.

4.1. **Hurwitz spaces of covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.** Two covers $f : X \to \mathbb{P}^1$ and $f' : X' \to \mathbb{P}^1$ are called **weakly equivalent** if there is a homeomorphism $h : X \to X'$ and an analytic automorphism g of $\mathbb{P}^1$ (i.e., a Moebius transformation) such that $g \circ f = f' \circ h$. The covers f and f' are called **equivalent** if the above holds with $g = 1$.

Consider a cover $f : X \to \mathbb{P}^1$ of degree n, with branch points $p_1, ..., p_r \in \mathbb{P}^1$. Pick $p \in \mathbb{P}^1 \setminus \{p_1, ..., p_r\}$, and choose loops γ_i around p_i such that $\gamma_1, ..., \gamma_r$ is a standard generating system of the fundamental group $\Gamma := \pi_1(\mathbb{P}^1 \setminus \{p_1, ..., p_r\}, p)$, in particular, we have $\gamma_1 \cdots \gamma_r = 1$. Such a system $\gamma_1, ..., \gamma_r$ is called a homotopy basis of $\mathbb{P}^1 \setminus \{p_1, ..., p_r\}$. The group Γ acts on the fiber $f^{-1}(p)$ by path lifting, inducing a transitive subgroup G of the symmetric group S_n (determined by f up to conjugacy in S_n). It is called the **monodromy group** of f. The images of $\gamma_1, ..., \gamma_r$ in S_n form a tuple of permutations $\sigma = (\sigma_1, ..., \sigma_r)$ called a tuple of **branch cycles** of f.

We say a cover $f : X \to \mathbb{P}^1$ of degree n is of type σ if it has σ as tuple of branch cycles relative to some homotopy basis of $\mathbb{P}^1$ minus the branch points of f. Let $\mathcal{H}_\sigma$ be the set of weak equivalence classes of covers of type σ. The **Hurwitz space** $\mathcal{H}_\sigma$ carries a natural structure of an quasiprojective variety.

We have $\mathcal{H}_\sigma = \mathcal{H}_\tau$ if and only if the tuples σ, τ are in the same **braid orbit** $\mathcal{O}_\tau = \mathcal{O}_\sigma$. In the case of the covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ from above, the corresponding braid orbit consists of all tuples in S_n whose cycle type matches the ramification structure of ϕ.

This and the genus of $\mathcal{H}_\sigma$ in the degenerate cases (see the following table) has been computed in GAP by the BRAID PACKAGE written by K. Magaard.

deg	Case	cycle type of σ	$\#(\mathcal{O}_\sigma)$	G	$\dim \mathcal{H}_\sigma$	genus of $\mathcal{H}_\sigma$
3		$(2^2, 2^2, 2^2, 2, 2)$	40	S_3	2	–
	1	$(2^2, 2^2, 4, 2)$	8	S_5	1	0
	2	$(2^2, 2^2, 2 \cdot 3, 2)$	6	S_5	1	0
	3	$(2^2, 2^2, 2^2, 3)$	9	A_5	1	1
	4					
5		$(2^2, 2^2, 2^2, 2, 2)$	40	S_5	2	–
	1	$(2^2, 2^2, 4, 2)$	8	S_5	1	0
	2	$(2^2, 2^2, 2 \cdot 3, 2)$	6	S_5	1	0
	3	$(2^2, 2^2, 2^2, 3)$	9	A_5	1	1
	4					
7		$(2^2, 2^2, 2^2, 2, 2)$	168	S_7	2	–

4.2. **Humbert surfaces.** Let $\mathcal{A}_2$ denote the moduli space of principally polarized abelian surfaces. It is well known that $\mathcal{A}_2$ is the quotient of the Siegel upper half space $\mathfrak{H}_2$ of symmetric complex 2×2 matrices with positive definite imaginary part by the action of the symplectic group $Sp_4(\mathbb{Z})$; see [11, p. 211].

Let Δ be a fixed positive integer and N_Δ be the set of matrices

$$\tau = \begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} \in \mathfrak{H}_2$$

such that there exist nonzero integers a, b, c, d, e with the following properties:

$$
\begin{aligned}
&az_1 + bz_2 + cz_3 + d(z_2^2 - z_1 z_3) + e = 0\\
&\Delta = b^2 - 4ac - 4de
\end{aligned} \tag{4}
$$

The *Humbert surface* $\mathcal{H}_\Delta$ of discriminant Δ is called the image of N_Δ under the canonical map

$$\mathfrak{H}_2 \to \mathcal{A}_2 := Sp_4(\mathbb{Z}) \setminus \mathfrak{H}_2,$$

see [14, 2, 24] for details. It is known that $\mathcal{H}_\Delta \neq \emptyset$ if and only if $\Delta > 0$ and $\Delta \equiv 0$ *or* $1 \mod 4$. Humbert (1900) studied the zero loci in Eq. (4) and discovered certain relations between points in these spaces and certain plane configurations of six lines; see [14] for more details.

For a genus 2 curve C defined over $\mathbb{C}$, $[C]$ belongs too $\mathcal{L}_n$ if and only if the isomorphism class $[J_C] \in \mathcal{A}_2$ of its (principally polarized) Jacobian J_C belongs to the Humbert surface $\mathcal{H}_{n^2}$, viewed as a subset of the moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces; see [24, Theorem 1, p. 125] for the proof of this statement. In [24] is shown that there is a one to one correspondence between the points in $\mathcal{L}_n$ and points in $\mathcal{H}_{n^2}$. Thus, we have the map:

$$
\begin{aligned}
\mathcal{H}_\sigma \ \longrightarrow\ &\mathcal{L}_n \ \longrightarrow\ \mathcal{H}_{n^2}\\
([f], (p_1, \dots, p_r)) \to &[\mathcal{X}] \to [J_{\mathcal{X}}]
\end{aligned} \tag{5}
$$

In particular, every point in $\mathcal{H}_{n^2}$ can be represented by an element of $\mathfrak{H}_2$ of the form

$$\tau = \begin{pmatrix} z_1 & \frac{1}{n} \\ \frac{1}{n} & z_2 \end{pmatrix}, \qquad z_1,\, z_2 \in \mathfrak{H}.$$

There have been many attempts to explicitly describe these Humbert surfaces. For some small discriminant this has been done by several authors; see [32], [26], [21]. Geometric characterizations of such spaces for $\Delta = 4, 8, 9,$ and 12 were given by Humbert (1900) in [14] and for $\Delta = 13, 16, 17, 20, 21$ by Birkenhake/Wilhelm (2003) in [2].

5. Genus 2 curves with degree 2 elliptic subcovers

An **elliptic involution** of K is an involution in G which is different from z_0 (the hyperelliptic involution). Thus the elliptic involutions of G are in 1-1 correspondence with the elliptic subfields of K of degree 2 (by the Riemann-Hurwitz formula).

If z_1 is an elliptic involution and z_0 the hyperelliptic one, then $z_2 := z_0\, z_1$ is another elliptic involution. So the elliptic involutions come naturally in pairs. This pairs also the elliptic subfields of K of degree 2. Two such subfields E_1 and E_2 are paired if and only if $E_1 \cap k(X) = E_2 \cap k(X)$. E_1 and E_2 are G-conjugate unless $G \cong D_6$ or $G \cong V_4$ (This can be checked from Lemma 1).

Theorem 3. *Let K be a genus 2 field and $e_2(K)$ the number of $Aut(K)$-classes of elliptic subfields of K of degree 2. Suppose $e_2(K) \geq 1$. Then the classical invariants*

of K satisfy the equation,

$$
\begin{aligned}
&-J_2^7J_4^4 + 8748J_{10}J_2^4J_6^2 507384000J_{10}^2J_4^2J_2 - 19245600J_{10}^2J_4J_2^3 - 592272J_{10}J_4^4J_2^2\\
&-81J_2^3J_6^4 - 3499200J_{10}J_2J_6^3 + 4743360J_{10}J_4^3J_2J_6 - 870912J_{10}J_4^2J_2^3J_6\\
&+1332J_2^4J_4^4J_6 - 125971200000J_{10}^3 + 384J_4^6J_6 + 41472J_{10}J_4^5 + 159J_4^6J_2^3\\
&-47952J_2J_4J_6^4 + 104976000J_{10}^2J_2^2J_6 - 1728J_4^5J_2^2J_6 + 6048J_4^4J_2J_6^2 + 108J_2^4J_4J_6^3\\
&+12J_2^6J_4^3J_6 + 29376J_2^2J_4^2J_6^3 - 8910J_2^3J_4^3J_6^2 - 2099520000J_{10}^2J_4J_6 - 236196J_{10}^2J_2^5\\
&+31104J_6^5 - 6912J_4^3J_6^34 + 972J_{10}J_2^6J_4^2 + 77436J_{10}J_4^3J_2^4 - 78J_2^5J_4^5\\
&+3090960J_{10}J_4J_2^2J_6^2 - 5832J_{10}J_2^5J_4J_6 - 80J_4^7J_2 - 54J_2^5J_4^2J_6^2 - 9331200J_{10}J_4^2J_6^2 = 0
\end{aligned}
\tag{6}
$$

Further, $e_2(K) = 2$ unless $K = k(X, Y)$ with

$$Y^2 = X^5 - X$$

in which case $e_2(K) = 1$.

Proof. Since $e_2(K)$ is the number of conjugacy classes of elliptic involutions in G the claim about $e_2(K)$ follows from theorem 5. For the proof of the following lemma see [32].

Lemma 5. *Suppose z_1 is an elliptic involution of K. Let $z_2 = z_1 z_0$, where z_0 is the hyperelliptic involution. Let E_i be the fixed field of z_i for $i = 1, 2$. Then $K = k(X, Y)$ where*

$$Y^2 = X^6 - s_1X^4 + s_2X^2 - 1 \tag{7}$$

and $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3 \neq 0$. Further E_1 and E_2 are the subfields $k(X^2, Y)$ and $k(X^2, YX)$.

We need to determine to what extent the normalization in the above proof determines the coordinate X. The condition $z_1(X) = -X$ determines the coordinate X up to a coordinate change by some $\gamma \in \Gamma$ centralizing z_1. Such γ satisfies $\gamma(X) = mX$ or $\gamma(X) = \frac{m}{X}$, $m \in k \setminus \{0\}$. The additional condition $abc = 1$ forces $1 = -\gamma(\alpha_1) \dots \gamma(a_6)$, hence $m^6 = 1$. So X is determined up to a coordinate change by the subgroup $H \cong D_6$ of Γ generated by $\tau_1 : X \to \xi_6 X$, $\tau_2 : X \to \frac{1}{X}$, where ξ_6 is a primitive 6-th root of unity. Let $\xi_3 := \xi_6^2$. The coordinate change by τ_1 replaces s_1 by $\xi_3 s_2$ and s_2 by $\xi_3^2 s_2$. The coordinate change by τ_2 switches s_1 and s_2. Invariants of this H-action are:

$$u := s_1s_2, \quad v := s_1^3 + s_2^3 \tag{8}$$

Remark 1. *Such invariants were quite important in simplifying computations for the locus $\mathcal{L}_2$. Later they have been used by Duursma and Kiyavash to show that genus 2 curves with extra involutions are suitable for the vector decomposition problem; see [7] for details. In this volume they are used again, see the paper by Cardona and Quer. They were later generalized to higher genus hyperelliptic curves and were called dihedral invariants; see [13].*

Classical invariants of the field K given by lemma 5 are:

$$
\begin{aligned}
J_2 &= 240 + 16u\\
J_4 &= 48v + 4u^2 + 1620 - 504u\\
J_6 &= -20664u + 96v - 424u^2 + 24u^3 + 160uv + 119880\\
J_{10} &= 64(27 - 18u - u^2 + 4v)^2
\end{aligned}
\tag{9}
$$

For $J_2 \neq 0$ we express the absolute invariants i_1, i_2, i_3 in terms of u and v. We can eliminate u and v and get the following equation of $\mathcal{L}_2$.

$$
\begin{aligned}
&-27i_1^6 + 9i_1^7 + 161243136 i_3 i_1^3 - 12441600 i_3 i_2^3 + 2i_2^5 + 107495424 i_3 i_1^2 i_2 + 54 i_1^3 i_2^2 \\
&-52254720 i_3 i_1 i_2^2 - 47278080 i_3 i_1^3 i_2 - 8294400 i_3 i_1^2 i_2^2 - 9459597312000 i_3^2 i_1^2 - 18 i_1^4 i_2^2 \\
&-240734712102912 i_3^2 + 111451255603200 i_3^2 i_1 + 20639121408000 i_3^2 i_2 - 55240704 i_3 i_1^4 \\
&+2i_1^6 i_2 - 4i_1^3 i_2^3 + 331776 i_3 i_1^5 - 27 i_2^4 - 2866544640000 i_3^2 i_1 i_2 + 161243136 i_3 i_2^2 + 9 i_1 i_2^4 \\
&-2641807540224000000 i_3^3 = 0
\end{aligned}
\tag{10}
$$

To get rid of the condition $J_2 \neq 0$ we multiply by J_2^5 to get the "projective" equation (6) of $\mathcal{L}_2$. This holds indeed for all $K \in \mathcal{L}_2$, as can be checked by substituting from (9). This completes the proof of Theorem 3.

$\square$

The following proposition determines the group G in terms of u and v.

Proposition 1. *Let $\mathcal{C}$ be a genus 2 curve such that $G := Aut(\mathcal{C})$ has an elliptic involution and $J_2 \neq 0$. Then,*

a) $G \cong \mathbb{Z}_3 \rtimes D_4$ if and only if $(u, v) = (0, 0)$ or $(u, v) = (225, 6750)$.

b) $G \cong W_1$ if and only if $u = 25$ and $v = -250$.

c) $G \cong D_6$ if and only if $4v - u^2 + 110u - 1125 = 0$, for $u \neq 9, 70 + 30\sqrt{5}, 25$. Moreover, the classical invariants satisfy the equations,

$$
\begin{aligned}
&-J_4 J_2^4 + 12 J_2^3 J_6 - 52 J_4^2 J_2^2 + 80 J_4^3 + 960 J_2 J_4 J_6 - 3600 J_6^2 = 0 \\
&864 J_{10} J_2^5 + 3456000 J_{10} J_4^2 J_2 - 43200 J_{10} J_4 J_2^3 - 2332800000 J_{10}^2 - J_4^2 J_2^6 \\
&-768 J_4^4 J_2^2 + 48 J_4^3 J_2^4 + 4096 J_4^5 = 0
\end{aligned}
\tag{11}
$$

d) $G \cong D_4$ if and only if $v^2 - 4u^3 = 0$, for $u \neq 1, 9, 0, 25, 225$. Cases $u = 0, 225$ and $u = 25$ are reduced to cases a),and b) respectively. Moreover, the classical invariants satisfy (6) and the following equation,

$$
1706 J_4^2 J_2^2 + 2560 J_4^3 + 27 J_4 J_2^4 - 81 J_2^3 J_6 - 14880 J_2 J_4 J_6 + 28800 J_6^2 = 0 \tag{12}
$$

Proposition 2. *The mapping*

$$
A : (u, v) \longrightarrow (i_1, i_2, i_3)
$$

gives a birational parametrization of $\mathcal{L}_2$. The fibers of A of cardinality > 1 correspond to those curves $\mathcal{C}$ with $|Aut(\mathcal{C})| > 4$.

Proof. See [32] for the details. $\square$

5.1. **Elliptic subcovers.** Let j_1 and j_2 denote the j-invariants of the elliptic curves E_1 and E_2 from lemma 5. The invariants j_1 and j_2 and are roots of the quadratic

$$
j^2 + 256 \frac{(2u^3 - 54u^2 + 9uv - v^2 + 27v)}{(u^2 + 18u - 4v - 27)} j + 65536 \frac{(u^2 + 9u - 3v)}{(u^2 + 18u - 4v - 27)^2} = 0 \tag{13}
$$

5.1.1. *Isomorphic elliptic subcovers.* The elliptic curves E_1 and E_2 are isomorphic when equation (13) has a double root. The discriminant of the quadratic is zero for

$$
(v^2 - 4u^3)(v - 9u + 27) = 0
$$

Remark 2. *From lemma 5, $v^2 = 4u^3$ if and only if $Aut(\mathcal{C}) \cong D_4$. So for $\mathcal{C}$ such that $Aut(\mathcal{C}) \cong D_4$, E_1 is isomorphic to E_2. It is easily checked that z_1 and $z_2 = z_0 z_1$ are conjugate when $G \cong D_4$. So they fix isomorphic subfields.*

If $v = 9(u-3)$ then the locus of these curves is given by,

$$
\begin{aligned}
4i_1^5 - 9i_1^4 + 73728 i_1^2 i_3 - 150994944 i_3^2 = 0 \\
289 i_1^3 - 729 i_1^2 + 54 i_1 i_2 - i_2^2 = 0
\end{aligned}
\tag{14}
$$

For $(u,v) = (\frac{9}{4}, -\frac{27}{4})$ the curve has $Aut(\mathcal{C}) \cong D_4$ and for $(u,v) = (137, 1206)$ it has $Aut(\mathcal{C}) \cong D_6$. All other curves with $v = 9(u-3)$ belong to the general case, so $Aut(\mathcal{C}) \cong V_4$. The j-invariants of elliptic curves are $j_1 = j_2 = 256(9-u)$. Thus, these genus 2 curves are parameterized by the j-invariant of the elliptic subcover.

Remark 3. *This embeds the moduli space $\mathcal{M}_1$ into $\mathcal{M}_2$ in a functorial way.*

5.2. **Isogenous degree 2 elliptic subfields.** In this section we study pairs of degree 2 elliptic subfields of K which are 2 or 3-isogenous. We denote by $\Phi_n(x,y)$ the n-th modular polynomial (see Blake et al. [1] for the formal definitions. Two elliptic curves with j-invariants j_1 and j_2 are n-isogenous if and only if $\Phi_n(j_1, j_2) = 0$.

5.2.1. *3-Isogeny.* Suppose E_1 and E_2 are 3-isogenous. Then, from equation (13) and $\Phi_3(j_1, j_2) = 0$ we eliminate j_1 and j_2. Then,

$$
(4v - u^2 + 110u - 1125) \cdot g_1(u,v) \cdot g_2(u,v) = 0 \tag{15}
$$

where g_1 and g_2 are

$$
\begin{aligned}
g_1 = & -27008u^6 + 256u^7 - 2432u^5v + v^4 + 7296u^3v^2 - 6692v^3u - 1755067500u \\
& + 2419308v^3 - 34553439u^4 + 127753092vu^2 + 16274844vu^3 - 1720730u^2v^2 \\
& - 1941120u^5 + 381631500v + 1018668150u^2 - 116158860u^3 + 52621974v^2 \\
& + 387712u^4v - 483963660vu - 33416676v^2u + 922640625
\end{aligned}
\tag{16}
$$

$$
\begin{aligned}
g_2 = & \ 291350448u^6 - v^4u^2 - 998848u^6v - 3456u^7v + 4749840u^4v^2 + 17032u^5v^2 \\
& + 4v^5 + 80368u^8 + 256u^9 + 6848224u^7 - 10535040v^3u^2 - 35872v^3u^3 + 26478v^4u \\
& - 77908736u^5v + 9516699v^4 + 307234984u^3v^2 - 419583744v^3u - 826436736v^3 \\
& + 27502903296u^4 + 28808773632vu^2 - 23429955456vu^3 + 5455334016u^2v^2 \\
& - 41278242816v + 82556485632u^2 - 108737593344u^3 - 12123095040v^2 \\
& + 41278242816vu + 3503554560v^2u + 5341019904u^5 - 2454612480u^4v
\end{aligned}
\tag{17}
$$

Thus, there is a isogeny of degree 3 between E_1 and E_2 if and only if u and v satisfy equation (15). The vanishing of the first factor is equivalent to $G \cong D_6$. So, if $Aut(\mathcal{C}) \cong D_6$ then E_1 and E_2 are isogenous of degree 3. This was also noted by Gaudry and Schost [10].

5.2.2. *2-Isogeny.* Below we give the modular 2-polynomial.

$$
\begin{aligned}
\Phi_2 = & \ x^3 - x^2y^2 + y^3 + 1488xy(x+y) + 40773375xy - 162000(x^2 - y^2) + \\
& 8748000000(x+y) - 157464000000000
\end{aligned}
\tag{18}
$$

Suppose E_1 and E_2 are isogenous of degree 2. Substituting j_1 and j_2 in Φ_2 we get

$$
f_1(u,v) \cdot f_2(u,v) = 0 \tag{19}
$$

where f_1 and f_2 are

$$
\begin{aligned}
f_1 = & -16v^3 - 81216v^2 - 892296v - 2460375 + 3312uv^2 + 707616vu + 3805380u + \\
& 18360vu^2 - 1296162u^2 - 1744u^3v - 140076u^3 + 801u^4 + 256u^5
\end{aligned}
\tag{20}
$$

$$
\begin{aligned}
f_2 = {} & 4096u^7 + 256016u^6 - 45824u^5v + 4736016u^5 - 2126736vu^4 + 23158143u^4 \\
& - 25451712u^3v - 119745540u^3 + 5291136v^2u^2 - 48166488vu^2 - 2390500350u^2 \\
& - 179712uv^3 + 35831808uv^2 + 1113270480vu + 9300217500u - 4036608v^3 \\
& - 1791153000v - 8303765625 - 1024v^4 + 163840u^3v^2 - 122250384v^2 + 256u^2v^3
\end{aligned} \tag{21}
$$

5.2.3. *Other isogenies between elliptic subcovers.* If $G \cong D_4$, then z_1 and z_2 are in the same conjugacy class. There are again two conjugacy classes of elliptic involutions in G. Thus, there are two degree 2 elliptic subfields (up to isomorphism) of K. One of them is determined by double root j of the equation (13), for $v^2 - 4u^3 = 0$. Next, we determine the j-invariant j' of the other degree 2 elliptic subfield and see how it is related to j.

$$
\begin{tikzcd}
 & & C \arrow[dll] \arrow[dl] \arrow[drr] \arrow[drrr] & & & \\
E_1 \arrow[r, squiggly, dash] & E_2 & & & E_1' \arrow[r, squiggly, dash] & E_2'
\end{tikzcd}
$$

If $v^2 - 4u^3 = 0$ then $\mathbf{G} \cong V_4$ and $\mathcal{P} = \{\pm 1, \pm\sqrt{a}, \pm\sqrt{b}\}$. Then, $s_1 = a + \frac{1}{a} + 1 = s_2$. Involutions of $\mathcal{C}$ are $\tau_1 : X \to -X$, $\tau_2 : X \to \frac{1}{X}$, $\tau_3 : X \to -\frac{1}{X}$. Since τ_1 and τ_3 fix no points of $\mathcal{P}$ the they lift to involutions in G. They each determine a pair of isomorphic elliptic subfields. The j-invariant of elliptic subfield fixed by τ_1 is the double root of equation (13), namely

$$j = -256 \frac{v^3}{v+1}$$

To find the j-invariant of the elliptic subfields fixed by τ_3 we look at the degree 2 covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, such that $\phi(\pm 1) = 0$, $\phi(a) = \phi(-\frac{1}{a}) = 1$, $\phi(-a) = \phi(\frac{1}{a}) = -1$, and $\phi(0) = \phi(\infty) = \infty$. This covering is, $\phi(X) = \frac{\sqrt{a}}{a-1} \frac{X^2-1}{X}$. The branch points of ϕ are $q_i = \pm \frac{2i\sqrt{a}}{\sqrt{a-1}}$. From lemma 5 the elliptic subfields E_1' and E_2' have 2-torsion points $\{0, 1, -1, q_i\}$. The j-invariants of E_1' and E_2' are

$$j' = -16 \frac{(v-15)^3}{(v+1)^2}$$

Then $\Phi_2(j, j') = 0$, so E_1 and E_1' are isogenous of degree 2. Thus, τ_1 and τ_3 determine degree 2 elliptic subfields which are 2-isogenous.

6. Genus 2 curves with degree 3 elliptic subcovers

This case was studied in detail in[26]. The main theorem was:

Theorem 4. *Let K be a genus 2 field and $e_3(K)$ the number of $Aut(K/k)$-classes of elliptic subfields of K of degree 3. Then;*

i) $e_3(K) = 0, 1, 2,$ *or* 4

ii) $e_3(K) \geq 1$ *if and only if the classical invariants of K satisfy the irreducible equation* $F(J_2, J_4, J_6, J_{10}) = 0$ *displayed in* [26, Appendix A].

There are exactly two genus 2 curves (up to isomorphism) with $e_3(K) = 4$. The case $e_3(K) = 1$ (resp., 2) occurs for a 1-dimensional (resp., 2-dimensional) family of genus 2 curves, see [26].

Lemma 6. *Let K be a genus 2 field and E an elliptic subfield of degree 3.*

i) Then $K = k(X,Y)$ such that

$$Y^2 = (4X^3 + b^2X^2 + 2bX + 1)(X^3 + aX^2 + bX + 1) \tag{22}$$

for $a, b \in k$ such that

$$(4a^3 + 27 - 18ab - a^2b^2 + 4b^3)(b^3 - 27) \neq 0 \tag{23}$$

The roots of the first (resp. second) cubic correspond to $W^{(1)}(K,E)$, (resp. $W^{(2)}(K,E)$) in the coordinates X, Y, (see theorem 1).

ii) $E = k(U,V)$ where

$$U = \frac{X^2}{X^3 + aX^2 + bX + 1}$$

and

$$V^2 = U^3 + 2\frac{ab^2 - 6a^2 + 9b}{R}U^2 + \frac{12a - b^2}{R}U - \frac{4}{R} \tag{24}$$

where $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3 \neq 0$.

iii) Define

$$u := ab, \quad v := b^3$$

Let K' be a genus 2 field and $E' \subset K'$ a degree 3 elliptic subfield. Let a', b' be the associated parameters as above and $u' := a'b'$, $v = (b')^3$. Then, there is a k-isomorphism $K \to K'$ mapping $E \to E'$ if and only if exists a third root of unity $\xi \in k$ with $a' = \xi a$ and $b' = \xi^2 b$. If $b \neq 0$ then such ξ exists if and only if $v = v'$ and $u = u'$.

iv) The classical invariants of K satisfy equation [26, Appendix A].

Let

$$\begin{aligned} F(X) &:= X^3 + aX^2 + bX + 1 \\ G(X) &:= 4X^3 + b^2X^2 + 2bX + 1 \end{aligned} \tag{25}$$

Denote by $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3$ the resultant of F and G. Then we have the following lemma.

Lemma 7. *Let $a, b \in k$ satisfy equation* (23). *Then equation* (22) *defines a genus 2 field $K = k(X,Y)$. It has elliptic subfields of degree 3, $E_i = k(U_i, V_i)$, $i = 1, 2$, where U_i, and V_i are as follows:*

$$U_1 = \frac{X^2}{F(X)}, \quad V_1 = Y\,\frac{X^3 - bX - 2}{F(X)^2}$$

$$U_2 = \begin{cases} \dfrac{(X-s)^2(X-t)}{G(X)} & if \quad b(b^3 - 4ba + 9) \neq 0 \\[2mm] \dfrac{(3X - a)}{3(4X^3 + 1)} & if \quad b = 0 \\[2mm] \dfrac{(bX+3)^2}{b^2G(X)} & if \quad (b^3 - 4ba + 9) = 0 \end{cases} \tag{26}$$

where

$$s = -\frac{3}{b}, \quad t = \frac{3a - b^2}{b^3 - 4ab + 9}$$

$$V_2 = \begin{cases} \frac{\sqrt{27-b^3}Y}{G(X)^2}((4ab-8-b^3)X^3-(b^2-4ab)X^2+bX+1) & if \quad b(b^3-4ba+9)\neq 0 \\ Y\frac{8X^3-4aX^2-1}{(4X^3+1)^2} & if \quad b=0 \\ \frac{8}{b}\sqrt{b}\frac{Y}{G(X)}(bX^3+9X^2+b^2X+b) & if \quad (b^3-4ba+9)=0 \end{cases} \tag{27}$$

Proof. We skip the details of the proof. ∎

6.1. **Function field of $\mathcal{L}_3$.** The absolute invariants i_1, i_2, and i_3 are expressed in terms of u, v. Let u, v be independent transcendentals over k and $i_1, i_2, i_3 \in k(u, v)$. Further elements $r_1, r_2 \in k(u, v)$ are defined below; see § 6.1.1.

From the resultants of equations if i_1, i_2, i_3 in terms of u, v, we determine that $[k(v) : k(i_1, i_2)] = 16$, $[k(v) : k(i_2, i_3)] = 40$, and $[k(v) : k(i_1, i_3)] = 26$. We also can show that $u \in k(i_1, i_2, i_3, v)$, the expression is large and we display it on [26, Appendix A]. Thus, $[k(u, v) : k(i_1, i_2, i_3)] \leq 2$, see figure 1.

$$\begin{tikzcd} & k(u,v) \arrow[d, dash, "2"'] & \\ & k(i_1,i_2,i_3)=k(r_1,r_2) \arrow[dl, dash, "8"'] \arrow[d, dash, "20"] \arrow[dr, dash, "13"] & \\ k(i_1,i_2) & k(i_1,i_3) & k(i_2,i_3) \end{tikzcd}$$

FIGURE 1.

Computing the equation [26, Appendix A] directly from the equations of i_1, i_2, i_3 in terms of u, v, exceeds available computer power. We use additional invariants r_1, r_2 to overcome this problem.

6.1.1. *Invariants of Two Cubics.* We define the following invariants of two cubic polynomials. For $F(X) = a_3X^3 + a_2X^2 + a_1X + a_0$ and $G(X) = b_3X^3 + b_2X^2 + b_1X + b_0$ define

$$H(F,G) := a_3b_0 - \frac{1}{3}a_2b_1 + \frac{1}{3}a_1b_2 - a_0b_3$$

We denote by $R(F, G)$ the resultant of F and G and by $D(F)$ the discriminant of F. Also,

$$r_1(F,G) = \frac{H(F,G)^3}{R(F,G)}, \quad r_2(F,G) = \frac{H(F,G)^4}{D(F)\,D(G)}$$

Remark 4. *Note that $D(FG) = D(F) \cdot D(G) \cdot R^2(F, G)$.*

For

$$F(X) = X^3 + aX^2 + bX + 1, \quad G(X) = 4X^3 + b^2X^2 + 2bX + 1$$

from lemma 6 we have

$$
\begin{aligned}
r_1(F,G) &= 27\frac{v(v-9-2u)^3}{4v^2-18uv+27v-u^2v+4u^3}\\
r_2(F,G) &= -1296\frac{v(v-9-2u)^4}{(v-27)(4v^2-18uv+27v-u^2v+4u^3)}
\end{aligned}
\tag{28}
$$

Remark 5. *Note that r_1, r_2 are defined for any u, v by* (23).

Taking the resultants from the above equations we get the following equations for u and v over $k(r_1, r_2)$:

$$
\begin{aligned}
&65536r_1r_2^3u^2 + (42467328r_2^4 + 21233664r_2^4r_1 + 480r_2r_1^4 + 2r_1^5 + 41472r_2^2r_1^3\\
&+1548288r_2^3r_1^2 - 294912r_2^3r_1)u - 382205952r_2^4 + 238878720r_2^4r_1 - 2654208r_2^3r_1\\
&+13934592r_2^3r_1^2 + 285696r_2^2r_1^3 + 2400r_2r_1^4 + 7r_1^5 = 0
\end{aligned}
\tag{29}
$$

$$
\begin{aligned}
&16384v^2r_2^3 + (221184r_2^3r_1 + r_1^4 + 11520r_2^2r_1^2 - 442368r_2^3 + 192r_2r_1^3)v\\
&-5971968r_2^3r_1 - 864r_2r_1^3 - 124416r_2^2r_1^2 - 2r_1^4 = 0
\end{aligned}
\tag{30}
$$

In equation (29) express r_1 and r_2 in terms of u and v. Roots of this equation are u and $\nu(u)$ where,

$$
\nu(u) = \frac{(v-3u)(324u^2+15u^2v-378uv-4uv^2+243v+72v^2)}{(v-27)(4u^3+27v-18uv-u^2v+4v^2)}
\tag{31}
$$

Similarly for v we get

$$
\nu(v) = -\frac{4(v-3u)^3}{4u^3+27v-18uv-u^2v+4v^2}
\tag{32}
$$

Define a ring homomorphism

$$
\nu : k[u,v] \to k(u,v)
$$

$$
u \to \nu(u), \quad v \to \nu(v)
$$

Then, we compute $\nu^2 = 1$. Thus, ν extends to an involutory automorphism of $k(u,v)$ which we again denote by ν. Since,

$$
\tau : k(u,v) \to k(u,v)
$$

$$
(u,v) \to (u, \nu(v))
$$

is not involutory, then $[k(u,v) : k(r_1,r_2)] = 2$ and $Gal_{k(u,v)/k(r_1,r_2)} = \langle \nu \rangle$.

Lemma 8. *The fields $k(i_1,i_2,i_3) = k(r_1,r_2)$ are the same.*

Remark 6. *To find the equation in* [26, Appendix A] *we eliminate r_1 and r_2 from the three equations of the above lemma. This equation has degree 8, 13, and 20 in i_1, i_2, i_3 respectively.*

Proof. **(Theorem 4)** The map

$$
\theta : (u,v) \to (i_1,i_2,i_3)
$$

generically has degree 2, by previous section. Denote the minors of the Jacobian matrix of θ by $M_1(u,v), M_2(u,v), M_3(u,v)$. The system

$$
(33) \qquad \begin{cases} M_1(u,v)=0 \\ M_2(u,v)=0 \\ M_3(u,v)=0 \end{cases}
$$

has solutions

$$
(34) \qquad 8v^3+27v^2-54uv^2-u^2v^2+108u^2v+4u^3v-108u^3=0
$$

and 7 further solutions which we display in the following table together with the corresponding values (i_1,i_2,i_3) and properties of the corresponding genus 2 field K.

(u,v)	(i_1,i_2,i_3)	$Aut(K)$	$e_3(K)$
$(-\frac{7}{2},2)$	$J_{10}=0$, no associated genus 2 field K		
$(-\frac{775}{8},\frac{125}{96})$, $(\frac{25}{2},\frac{250}{9})$	$-\frac{8019}{20},-\frac{1240029}{200},\frac{531441}{100000}$	D_4	2
$(27-\frac{77}{2}\sqrt{-1},23+\frac{77}{9}\sqrt{-1})$, $(27+\frac{77}{2}\sqrt{-1},23-\frac{77}{9}\sqrt{-1})$	$(\frac{729}{2116},\frac{1240029}{97336},\frac{531441}{13181630464}$	D_4	2
$(-15+\frac{35}{8}\sqrt{5},\frac{25}{2}+\frac{35}{6}\sqrt{5})$, $(-15-\frac{35}{8}\sqrt{5},\frac{25}{2}-\frac{35}{6}\sqrt{5})$	$81,-\frac{5103}{25},-\frac{729}{12500}$	D_6	2

FIGURE 2. Corresponding (u,v) for which the Jacobian matrix of θ is 0

Assume that equation (34) holds for some $(u,v)\in k^2$. Then the corresponding quantities J_{2i}, $i=1,2,3,5$ satisfy the equation

$$
(35) \qquad F(J_2,J_4,J_6,J_{10})=0
$$

where $F(J_2,J_4,J_6,J_{10})$ is displayed in [26]. This is obtained by taking the resultants of equations of i_1,i_2,i_3 and (34). We define $J_{48}:=F(J_2,J_4,J_6,J_{10})$. By previous section θ is generically a covering of degree 2. So exists a Zariski open subset $\mathcal{U}$ of k^2 with the following properties: Firstly, θ is defined everywhere on $\mathcal{U}$ and is a covering of degree 2 from $\mathcal{U}$ to $\theta(\mathcal{U})$. Further, if $\mathfrak{u}\in\mathcal{U}$ then all $\mathfrak{u}'\in k^2$ with θ defined at $\mathfrak{u}'$ and $\theta(\mathfrak{u}')=\theta(\mathfrak{u})$ also lie in $\mathcal{U}$. Suppose $\underline{i}\in k^3$ such that $|\theta^{-1}(\underline{i})|>2$ and $det(Jac(\theta))$ does not vanish at any point of $\theta^{-1}(\underline{i})$. Then by implicit function theorem, there is an open ball B around each element of $\theta^{-1}(\underline{i})$ such that each point in $\theta(B)$ has >2 inverse images under θ. But B has to intersect the Zariski open set $\mathcal{U}$. This is a contradiction. Thus, if $\underline{i}\in k^3$ and $|\theta^{-1}(\underline{i})|>2$, then $det(Jac(\theta))=0$ at some point of $\theta^{-1}(\underline{i})$ and so J_{48} vanishes.

Let $e_3(K)>1$ and $J_2\neq 0$, $J_{48}\neq 0$. Then i_1,i_2,i_3 are defined and by previous paragraph $|\theta^{-1}(i_1,i_2,i_3)|\leq 2$. Thus, by lemma 6 part iii) $e_3(K)\leq 2$. This completes the proof of theorem 4.

□

6.2. **Elliptic subcovers.** We express the j-invariants j_i of the elliptic subfields E_i of K, from lemma 7, in terms of u and v as follows:

$$
\begin{aligned}
j_1 &= 16v\frac{(vu^2+216u^2-126vu-972u+12v^2+405v)^3}{(v-27)^3(4v^2+27v+4u^3-18vu-vu^2)^2}\\
j_2 &= -256\frac{(u^2-3v)^3}{v(4v^2+27v+4u^3-18vu-vu^2)}
\end{aligned}
\tag{36}
$$

where $v \neq 0, 27$.

Remark 7. *The automorphism $\nu \in Gal_{k(u,v)/k(r_1,r_2)}$ permutes the elliptic subfields. One can easily check that:*

$$\nu(j_1) = j_2, \quad \nu(j_2) = j_1$$

Define T and N as follows;

$$
\begin{aligned}
T =& \frac{1}{16777216r_2^3r_1^8}(1712282664960r_2^3r_1^6 + 1528823808r_2^4r_1^6 + 49941577728r_2^4r_1^5\\
&- 38928384r_2^5r_1^5 - 258048r_2^6r_1^4 + 12386304r_2^6r_1^3 + 901736973729792r_2r_1^{10}\\
&+ 966131712r_2^5r_1^4 + 16231265527136256r_1^{10} + 480r_2^8r_1 + 101376r_2^7r_1^2 + 479047767293952r_2r_1^8\\
&+ 7247757312r_2^3r_1^8 + 7827577896960r_2^2r_1^9 + 2705210921189376r_1^9 + 619683250176r_2^3r_1^7\\
&+ 21641687369515008r_1^{12} + 3246253105427251 2r_1^{11} + r_2^9 + 37572373905408r_2^2r_1^7\\
&+ 1408964021452800r_2r_1^9 + 45595641249792r_2^2r_1^8)\\
N =& -\frac{1}{68719476736r_1^12r_2^3}(84934656r_1^5 + 1179648r_1^4r_2 - 5308416r_1^4 - 442368r_1^3r_2\\
&- 13824r_1^2r_2^2 - 192r_1r_2^3 - r_2^4)^3
\end{aligned}
\tag{37}
$$

Lemma 9. *The j-invariants of the elliptic subfields satisfy the following quadratic equations over $k(r_1, r_2)$;*

$$j^2 - T\,j + N = 0 \tag{38}$$

Proof. Substitute j_1 and j_2 as in (36) in equation (38). □

6.2.1. *Isomorphic Elliptic Subfields.* Suppose that $E_1 \cong E_2$. Then, $j_1 = j_2$ implies that

$$8v^3 + 27v^2 - 54uv^2 - u^2v^2 + 108u^2v + 4u^3v - 108u^3 = 0 \tag{39}$$

or

$$
\begin{aligned}
&324v^4u^2 - 5832v^4u + 37908v^4 - 314928v^3u - 81v^3u^4 + 255879v^3 + 30618v^3u^2\\
&- 864v^3u^3 - 6377292uv^2 + 8503056v^2 - 324u^5v^2 + 2125764u^2v^2 - 215784u^3v^2\\
&+ 14580u^4v^2 + 16u^6v^2 + 78732u^3v + 8748u^5v - 864u^6v - 157464u^4v + 11664u^6 = 0
\end{aligned}
\tag{40}
$$

The former equation is the condition that $det(Jac(\theta)) = 0$ see (35). From equation 35 and expressions of i_1, i_2, i_3 we can express u as a rational function in i_1, i_2, and v. This is displayed in [26, Appendix B]. Also, $[k(v) : k(i_1)] = 8$ and $[k(v) : k(i_2)] = 12$. Eliminating v we get a curve in i_1 and i_2 which has degree 8 and 12 respectively. Thus, $k(u, v) = k(i_1, i_2)$. Hence, $e_3(K) = 1$ for any K such that the associated u and v satisfy equation (35).

6.2.2. *The Degenerate Case.* We assume now that one of the extensions K/E_i from lemma 7 is degenerate, i.e. has only one branch point. The following lemma determines a relation between j_1 and j_2.

Lemma 10. *Suppose that K/E_2 has only one branch point. Then,*

$$729 j_1 j_2 - (j_2 - 432)^3 = 0$$

Making the substitution $T = -27 j_1$ we get

$$j_1 = F_2(T) = \frac{(T+16)^3}{T}$$

where $F_2(T)$ is the Fricke polynomial of level 2.

If both K/E_1 and K/E_2 are degenerate then

$$\begin{cases} 729 j_1 j_2 - (j_1 - 432)^3 = 0 \\ 729 j_1 j_2 - (j_2 - 432)^3 = 0 \end{cases} \tag{41}$$

There are 7 solutions to the above system. Three of which give isomorphic elliptic curves

$$j_1 = j_2 = 1728, \quad j_1 = j_2 = \frac{1}{2}(297 \pm 81\sqrt{-15})$$

The other 4 solutions are given by:

$$\begin{cases} 729 j_1 j_2 - (j_1 - 432)^3 = 0 \\ j_1^2 + j_2^2 - 1296(j_1 + j_2) + j_1 j_2 + 559872 = 0 \end{cases} \tag{42}$$

This corrects [21] where it is claimed there is only one solution $j_1 = j_2 = 1728$.

7. Further remarks

If $e_3(\mathcal{C}) \geq 1$ then the automorphism group of $\mathcal{C}$ is one of the following: $\mathbb{Z}_2, V_4$, D_4, or D_6. Moreover; there are exactly 6 curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_4 and six curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_6. They are listed in [29] where rational points of such curves are found.

Genus 2 curves with degree 5 elliptic subcovers are studied in [33] where a description of the space $\mathcal{L}_5$ is given and all its degenerate loci. The case of degree 7 is the first case when all possible degenerate loci occur.

We have organized the results of this paper in a Maple package which determines if a genus 2 curve has degree $n = 2, 3$ elliptic subcovers. Further, all its elliptic subcovers are determined explicitly. We intend to implement the results for $n = 5$ and the degenerate cases for $n = 7$.

References

[1] I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, LMS, 265, (1999).

[2] C. Birkenhake, H. Wilhelm, Humbert surfaces and the Kummer plane. Trans. Amer. Math. Soc. 355 (2003), no. 5, 1819–1841.

[3] O. Bolza, On binary sextics with linear transformations into themselves. *Amer. J. Math.* **10**, 47-70.

[4] R. Brandt, Über Die Automorphismengruppen von algebraischen Funktionenkörpern, (unpublished) PhD thesis. Universität-Gesamthochschule Essen, 1988.

[5] R. Brandt and H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, *Man. Math.* 55, 83-92, 1986.

[6] A. Clebsch, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig, 1872.

[7] I. Duursma and N. Kiyavash, The Vector Decomposition Problem for Elliptic and Hyperelliptic Curves, (preprint)

[8] G. Frey, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993)*, 79-98, Ser. Number Theory, I, *Internat. Press, Cambridge, MA*, 1995.

[9] G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetic application. *Arithmetic algebraic geometry (Texel, 1989)*, 153-176, *Progr. Math.*, 89, Birkhäuser Boston, MA, 1991.

[10] P. Gaudry and E. Schost, Invariants des quotients de la Jacobienne d'une courbe de genre 2, (in press)

[11] G. van der Geer, Hilbert modular surfaces, Springer, Berlin, 1987.

[12] Geyer W. Geyer, Invarianten binärer Formen, *Lecture Notes in Math.*, Springer, New York, (1972).

[13] J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, *LMS J. of Comput. Math.*, 8 (2005), 102-115.

[14] G. Humbert Sur les fonctionnes abliennes singulires. I, II, III. J. Math. Pures Appl. serie 5, t. V, 233–350 (1899); t. VI, 279–386 (1900); t. VII, 97–123 (1901).

[15] J. Igusa, Arithmetic Variety Moduli for genus 2. *Ann. of Math.* (2), 72, 612-649, 1960.

[16] C. Jacobi, Review of Legendre, Théorie des fonctions elliptiques. Troiseme supplém ent. 1832. J. reine angew. Math. 8, 413-417.

[17] E, Kani and W. Schanz, Diagonal quotient surfaces. Manuscripta Math. 93, no. 1, 67–108, 1997.

[18] E. Kani, The number of curves of genus two with elliptic differentials. J. Reine Angew. Math. 485 (1997), 93–121.

[19] A. Krazer, Lehrbuch der Thetafunctionen, Chelsea, New York, 1970.

[20] V. Krishnamorthy, T. Shaska, H. Völklein, Invariants of binary forms , *Developments in Mathematics*, Vol. 12, Springer 2005, pg. 101-122.

[21] M. R. Kuhn, Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc* **307**, 41-49, 1988.

[22] H. Lange, Über die Modulvarietät der Kurven vom Geschlecht 2. *J. Reine Angew. Math.*, 281, 80-96, 1976.

[23] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group. *Communications in arithmetic fundamental groups* (Kyoto, 1999/2001). Sūrikaisekikenkyūsho Kōkyūroku No. 1267 (2002), 112–141.

[24] N. Murabayashi, The moduli space of curves of genus two covering elliptic curves. Manuscripta Math. 84 (1994), no. 2, 125–133.

[25] D. Sevilla, T. Shaska, Hyperelliptic curves with reduced automorphism group A_5, (submitted).

[26] T. Shaska, Genus 2 curves with degree 3 elliptic subcovers, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[27] T. Shaska, Some special families of hyperelliptic curves, *J. Algebra Appl.*, vol **3**, No. 1 (2004), 75-89.

[28] T. Shaska, Computational algebra and algebraic curves, ACM, *SIGSAM Bulletin*, *Comm. Comp. Alg.*, Vol. **37**, No. 4, 117-124, 2003.

[29] T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, Algorithmic Number Theory (Sydney, 2002), **6**, 205-218, *Lect. Not. in Comp. Sci.*, 2369, Springer, Berlin, 2002.

[30] T. Shaska, Curves of genus 2 with (n, n)-decomposable Jacobians, *J. Symbolic Comput.* 31 (2001), no. 5, 603–617.

[31] T. Shaska and J. L. Thompson, On the generic curves of genus 3, *Affine Algebraic Geometry*, Cont. Math., American Mathematical Society, (2004).

[32] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications*, pg. 687 - 707, Springer (2004).

[33] T. Shaska, H. Völklein, Genus 2 curves with degree 5 elliptic subcovers, (preprint).

[34] G. Tamme, Ein Satz über hyperelliptische Funktionenkörper. J. Reine Angew. Math. 257, 217–220, 1972.

Department of Mathematics, Oakland University, Rochester, MI, 48309-4485.
E-mail address: shaska@oakland.edu